AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A data storage device comprising:

a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and

cryptosystem means;

wherein said cryptosystem means receives[[, as]] cryptosystem keys for performing cryptosystem processing on data to be stored in said data storage area, wherein the cryptosystem keys comprise:

a first set of keys ~~correlated with~~ comprising a plurality of encryption/decryption ~~the encryption~~ keys, each of the encryption/decryption keys corresponding to a particular sector and used to encrypt or decrypt that particular sector, ~~or decryption keys~~ for each of the sectors from a device capable of performing data communication with said data storage device, and

a second set of keys ~~correlated with~~ corresponding to integrity-check-value generating keys, the integrity-check-value generating keys being used to check the integrity of data to be stored in at least one of the sectors; and

wherein the first and second set of keys are encrypted in a cipher block chaining (CBC) mode by said ~~encryption~~ cryptosystem means ~~further creates encrypted keys by~~

~~executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode~~ using a storage key stored in said data storage device, and

transmits the encrypted keys to said data storage device.

2. (Original) A data storage device according to claim 1, wherein said cryptosystem means generates key data as the header information of the data to be stored in said data storage area by using a storage key which is unique to said data storage device to execute the encryption processing in the CBC mode on the received set of keys.

3. (Original) A data storage device according to claim 1, wherein:

said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is a set of session-key-used CBC-mode-processing keys encrypted in the CBC mode by using a session key generated in the mutual authentication;

said cryptosystem means performs the decryption in the CBC mode of said set of encrypted session-key-used CBC-mode-processing keys; and

in said cryptosystem means, a set of storage-key-used CBC-mode-processing keys is generated by executing, based on a storage key unique to said data storage device, the encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode processing keys, and said set of storage-key-used

CBC-mode-processing keys is transmitted as header-information-forming data to said device.

4. (Original) A data storage device according to claim 1, wherein:

said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is header information on the data to be stored in said data storage area, and is a set of storage-key-used CBC-mode-processing keys encrypted in the CBC mode based on a storage key unique to said data storage device;

said cryptosystem means performs the decryption in the CBC mode of the set of encrypted storage-key-used CBC-mode-processing keys by using said storage key; and

in said cryptosystem means, a set of session-key-used CBC-mode-processing keys is generated by executing, based on a session key generated in the mutual authentication, the encryption processing in the CBC mode, and said set of session-key-used CBC mode-processing keys is transmitted as data constituting decrypting key information.

5. (Canceled)

6. (Currently Amended) A data recording method for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data recording device for

executing data storage processing by transmitting data to said data storage device, said data recording method comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on a first set of keys ~~applicable~~ comprising a plurality of encryption keys, each of the encryption keys corresponding to a particular sector and used to encrypt ~~to encryption processing~~ on pieces of data to be stored in each of the particular sectors, and a second set of keys ~~correlating~~ corresponding to integrity-check-value generating keys, the integrity-check-value generating keys being used to check the integrity of data to be stored in at least one of the sectors, the encryption processing ~~being executed on~~ comprising encrypting said first and second set of keys in the CBC mode using a storage key stored in said data storage device;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key;

transmitting, to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set decrypted session-key-used CBC-mode-processing keys; and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device.

7. (Currently Amended) A data playback method for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playing back data which is received from said data storage device, said data playback method comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device;

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device on an integrity-check-value generating key, the integrity-check-value generating key being used to check the integrity of data to be stored in at least one of the sectors;

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key;

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by ~~executing,~~

encrypting the set of decrypted storage-key-used CBC-mode-processing keys in the CBC mode based on a session key generated in the mutual authentication~~, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys~~; and

obtaining, by said data playback device, a set of keys comprising a plurality of decryption keys, each of the decryption keys corresponding to a particular sector and used for decrypting encrypted sector data which is stored in each of the particular sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key.

8. (Currently Amended) A program providing medium for providing a computer program which controls a computer system to execute data recording processing for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data recording device for executing data storage processing by transmitting data to said data storage device, said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode processing keys which are generated by ~~executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on~~ encrypting a first set

of keys ~~applicable~~ comprising a plurality of encryption keys, each of the encryption keys corresponding to a particular sector and used to encrypt ~~to encryption processing~~ on pieces of data to be stored in each of the particular sectors, and a second set of keys ~~correlated with~~ corresponding to integrity-check-value generating keys of data, the integrity-check-value generating keys being used to check the integrity to be stored in at least one of the sectors, in the CBC mode based on a session key generated in the mutual authentication~~, the encryption processing being executed~~ using a storage key stored in said data storage device;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key;

transmitting, to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys; and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys; the header information corresponding to the data to be stored in said data storage device.

9. (Currently Amended) A program providing medium for providing a computer program which controls a computer system to execute data playback processing for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of

which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playback device data which is received from said data storage device; said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device;

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device on an integrity-check-value generating key, the integrity-check-value generating keys being used to check the integrity of data to be stored in at least one of the sectors;

decrypting, by said data storage device, the set of storage-key-used CBC--mode-processing keys by performing decryption in the CBC mode using the storage key;

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by ~~executing~~ encrypting the set of decrypted storage-key-used CBC-mode-processing keys[[,]] in the CBC mode based on a session key generated in the mutual authentication~~, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys~~; and

obtaining, by said data playback device, a set of keys comprising a plurality of decryption keys, each of the decryption keys corresponding to a particular sector and used for decrypting encrypted sector data which is stored in each of the particular

sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key.